IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION of	:	
Mistuhiro WATANABE	:	
Serial No.: [NEW]	:	Attn: Applications Branch
Filed: October 21, 2003	:	Attorney Docket No.: OKI.592

For: MICROCOMPUTER AND TEST METHOD THEREFOR

CLAIM OF PRIORITY

Honorable Assistant Commissioner for Patents and Trademarks,
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant, in the above-identified application, hereby claims the priority date under the International Convention of the following Japanese application:

Appln. No. 2002-354726 filed December 6, 2002

as acknowledged in the Declaration of the subject application.

A certified copy of said application is being submitted herewith.

Respectfully submitted,

VOLENTINE FRANCOS, PLLC

Adam C. Volentine
Registration No. 33,289

12200 Sunrise Valley Drive, Suite 150
Reston, Virginia 20191
Tel. (703) 715-0870
Fax. (703) 715-0877

Date: October 21, 2003

F-01ED0326-US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１２月 ６日

出 願 番 号
Application Number: 特願２００２－３５４７２６

[ST. 10/C]: [ＪＰ２００２－３５４７２６]

出 願 人
Applicant(s): 沖電気工業株式会社

２００３年 ８月２１日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０６８４９５

【書類名】　特許願
【整理番号】　KA003842
【提出日】　平成14年12月 6日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G01R 31/28
G06F 11/22
【発明者】
【住所又は居所】　東京都港区虎ノ門１丁目７番１２号　沖電気工業株式会社内
【氏名】　渡辺　充博
【特許出願人】
【識別番号】　000000295
【氏名又は名称】　沖電気工業株式会社
【代理人】
【識別番号】　100086807
【弁理士】
【氏名又は名称】　柿本　恭成
【手数料の表示】
【予納台帳番号】　007412
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9001054
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　マイクロコンピュータとその試験方法

【特許請求の範囲】

【請求項１】　通常動作用のプログラムが格納された第１のメモリと、

機能試験用のプログラムが格納された第２のメモリと、

外部端子から与えられる信号を監視して試験モードが指定されたことを検出する試験モード検出回路と、

前記試験モードが指定されていないときには前記第１のメモリにアクセスして前記通常動作用のプログラムを実行し、該試験モードが指定されたときには前記第２のメモリにアクセスして前記機能試験用のプログラムを実行する中央演算処理装置と、

前記第１及び第２のメモリに対するアクセスアドレス及びデータを監視し、許可されていない不正なアクセスがあったときに前記中央演算処理装置に対して特定の動作を実行させるメモリ管理ユニットと、

前記試験モード時に前記中央演算処理装置からセキュリティ試験信号が出力され、かつ特定のメモリ領域がアクセスされたときに、予め設定された特定の命令を該中央演算処理装置に与える試験回路とを、

備えたことを特徴とするマイクロコンピュータ。

【請求項２】　前記試験回路から前記中央演算処理装置に与える特定の命令は、前記メモリ管理ユニットで不正なアクセスとして検出される命令であることを特徴とする請求項１記載のマイクロコンピュータ。

【請求項３】　通常動作用のプログラムが格納された第１のメモリと、機能試験用のプログラムが格納された第２のメモリと、外部端子から与えられる信号を監視して試験モードが指定されたことを検出する試験モード検出回路と、前記試験モードが指定されていないときには前記第１のメモリにアクセスして前記通常動作用のプログラムを実行し、該試験モードが指定されたときには前記第２のメモリにアクセスして前記機能試験用のプログラムを実行する中央演算処理装置と、前記第１及び第２のメモリに対するアクセスアドレス及びデータを監視し、許可されていない不正なアクセスがあったときに前記中央演算処理装置に対して

特定の動作を実行させるメモリ管理ユニットとを備えたマイクロコンピュータにおいて、

前記中央処理装置は、前記機能試験用のプログラムによってセキュリティ試験が実行されており、かつ前記前記メモリ管理ユニットから前記特定の動作の実行が指示されたときに、所定の例外処理を行う例外処理回路を有することを特徴とするマイクロコンピュータ。

【請求項４】　プログラムを格納するメモリと、前記メモリに格納されたプログラムを実行する中央演算処理装置と、前記メモリに対するアクセスを監視して不正なアクセスを検出したときに前記中央演算処理装置に対して割り込み信号を出力するメモリ管理ユニットとを有するマイクロコンピュータの試験方法であって、

前記メモリの第１のアドレスに第２のアドレスへの分岐命令を書き込む処理と、

前記メモリ管理ユニットに対して、前記第２のアドレスの実行を不正なアクセスとして設定する処理と、

前記第１のアドレスに分岐する処理と、

前記第１のアドレスに書き込まれた分岐命令の実行の結果、前記メモリ管理ユニットから前記割り込み信号が出力されたか否かによって故障の有無を判定する処理とを、

順次実行することを特徴とするマイクロコンピュータの試験方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＩＣカードのようにセキュリティ機能を有するマイクロコンピュータ、特にそのセキュリティ機能を試験するための試験回路を備えたマイクロコンピュータとその試験方法に関するものである。

【０００２】

【従来の技術】

【０００３】

【特許文献１】

特開平０６－３２４９７２号公報

【特許文献２】

特開平０８－２７２６９５号公報

【０００４】

一般にＬＳＩ（大規模集積回路）は、シリコンウエハ上に微細な加工をしたりチップをパッケージに組み立てる製造過程において、ある確率で製造欠陥による動作不良品が発生する。従って、製造時に、出来上がったＬＳＩに電源と信号を印加し、期待どおりの動作をするか否かの試験を行って不良品を除去する。このため、可制御性・可観測性を向上させる目的で、ＬＳＩの論理設計時にスキャン機能等の試験回路を予め組み込んでおく試験容易化設計が行われている。

【０００５】

ここで、可制御性とは、ＬＳＩ内部の任意の信号を任意のレベル（“H”または“L”）に設定できることであり、可観測性とは、このＬＳＩ内部の任意の信号のレベルを検出できることである。すべての信号のレベルをＬＳＩの外部に出力して直接検出することは不可能なので、スキャン機能では、内部信号のレベルの変化を特定の端子の出力パターンの変化として出力させるような構成が採用されている。

【０００６】

しかし、可制御性・可観測性を高くすることは、内部信号を制御・検出できるということであり、セキュリティに関連するＬＳＩでは、そのセキュリティのレベルを下げることになる。パスワードや秘密鍵のように他人に知られてはならないデータを読み出されてしまうおそれがあるからである。

【０００７】

特に、ＩＣカード用のマイクロコンピュータでは、ＩＳＯ７８１６の規格で、端子形状と信号の電気的特性が規定され、外部接続用の端子は、電源（ＶＤＤ，ＧＮＤ）、クロック（ＣＬＫ）、リセット（ＲＳＴ）、及び半二重通信用の直列データ（ＳＩＯ）の５端子のみに限定されている。このようなマイクロコンピュータは、セキュリティ用途であることと、外部接続用の端子数が少ないことから

、試験に関して種々の制約がある。

【０００８】

更に、外部からアプリケーション・プログラムをダウンロードして実行できる高機能なセキュリティ向けのマイクロコンピュータでは、不正なプログラムがダウンロードされてパスワードや秘密鍵のデータを読み書きするような処理から保護するために、アプリケーション・プログラムにおける特定命令の実行や、特定領域へのアクセス及び分岐等を禁止するような高度のセキュリティ機能が必要である。

【０００９】

図２は、上記の機能を備えた従来のマイクロコンピュータの一例を示す構成図である。

【００１０】

このマイクロコンピュータは、ＣＰＵ（中央演算処理装置）１、ＲＯＭ（不揮発性メモリ）２，３、ＲＡＭ（随時読み書き可能メモリ）４、周辺回路５、バス（またはブリッジ）６、セキュリティ回路７、試験用回路８、及び試験モード検出回路９を備えている。

【００１１】

ＣＰＵ１は、ＲＯＭ２，３等のメモリに格納された命令を逐次実行するものである。ＲＯＭ２は、このマイクロコンピュータの主要な動作を決めるＯＳ（オペレーティング・システム）等のプログラムを格納したメモリである。ＲＯＭ３は、チップの製造試験用のプログラム、セキュリティ用の最小限のライブラリ、ファンクションコール用のサブルーチン等を格納したメモリである。

【００１２】

ＲＡＭ４は、データを格納したりプログラムを一時的に格納するためのメモリで、電気的に書き換え可能な不揮発性メモリも含まれる。周辺回路５は、暗号処理や外部との通信を行うための回路である。バス６は、ＣＰＵ１とその他のＲＯＭ２，３等の回路との接続部分で、トライステートバスやＯＲバスといったバス接続やブロック間の論理やタイミングを調整するブリッジ回路が用いられる。

【００１３】

セキュリティ回路７は、ＣＰＵ１が読み出したアドレスや命令を逐次監視し、実行や読み書きが許可されていないプログラム領域やデータ領域へのアクセスがあった場合に、ＣＰＵ１に対して不正アクセク検出信号ＩＬを出力して、適切な処理を行わせるための回路である。

【００１４】

試験用回路８は、チップ上に設けられて外部には接続されていない複数の試験信号入力端子８ａと、試験モード信号ＴＭで切り替え制御されるセレクタ８ｂを有している。試験用回路８は、製造試験時に試験装置のプローブを介して試験信号入力端子８ａからＣＰＵ１に試験用の命令を与え、任意の命令系列を実行させて、アプリケーション・プログラムを正しく実行できるか否か、或いは周辺回路５が正しく動作するか否かを試験する回路である。

【００１５】

試験モード検出回路９は、端子ＣＬＫ，ＲＳＴ，ＳＩＯに与えられる特定シーケンスの信号パターンを検出して、このマイクロコンピュータが試験モードに設定されたことを示すために、試験用回路８に対する試験モード信号ＴＭをアクティブにするものである。

【００１６】

次に動作を説明する。

【００１７】

このようなマイクロコンピュータにおいて製造時に行われる試験動作では、端子ＣＬＫ，ＲＳＴ，ＳＩＯに試験モードを設定するための特定の信号パターンが与えられる。これにより、試験モード検出回路９から出力される試験モード信号ＴＭがアクティブにされ、試験用回路８の試験信号入力端子８ａがＣＰＵ１に接続される。更に、外部の試験装置から試験信号入力端子８ａに試験用の命令を与え、ＣＰＵ１に任意の命令系列を実行させてユーザアプリケーションを正しく実行できるか否か、或いは周辺回路５が正しく動作するか否かを試験する。

【００１８】

一方、通常動作時には、ＣＰＵ１から出力されたアドレスＡＤＲは、セキュリティ回路７によって常に監視され、アクセスが許可された領域内か否かの判別が

行われる。実行が許可された領域であれば、ＲＯＭ２，３等のメモリから読み出された命令は、ＣＰＵ１によってそのまま実行される。実行が禁止された領域であれば、セキュリティ回路７から不正アクセク検出信号ＩＬが出力され、ＣＰＵ１によってプログラムの実行の中断や、アクセスの無効化等の処理が行われる。

【００１９】

【発明が解決しようとする課題】

しかしながら、従来のマイクロコンピュータでは、次のような課題があった。

【００２０】

（ａ）　試験用回路８は、外部の試験装置から試験用の命令を与えるための試験信号入力端子８ａを有している。この試験信号入力端子８ａは、外部の入出力ピンには接続されていないが、チップ上に試験用のパッドとして形成されているため、悪意ある第３者によって、そのパッドを介してデータを読み出したり、不正なプログラムをダウンロードする等のセキュリティの侵害が行われる危険性がある。

【００２１】

（ｂ）　不正アクセク検出信号ＩＬの配線パターンが電源のＧＮＤやＶＤＤとショートしていたり、セキュリティ回路７からこの不正アクセク検出信号ＩＬを出力するトランジスタの動作不良で、不正アクセク検出信号ＩＬが正しく出力されていないことを検出することができない。この理由は、次のとおりである。

【００２２】

ＲＯＭ３に格納した試験プログラムに基づいてＣＰＵ１がセキュリティ機能を自己試験し、不良の有無を端子ＣＬＫ，ＲＳＴ，ＳＩＯから出力する必要がある。これには、例えばＲＡＭ４に格納されたユーザアプリケーションによって、例外状態（不正な命令実行を検出した状態）を起こさせてそれが検出できるか、及び適正な動作時に例外状態が発生しないかを、分岐先のプログラムを実行することなく、試験用プログラムの実行の流れや読み出しデータの変化として、ＣＰＵ１で検出しなければならない。ここで、分岐先プログラムを実行することができないのは、ＲＯＭ２にはＯＳが格納されており、どのアドレスにどの命令が格納されているかを特定できないため、もし実行するとその後のＣＰＵ１の動作も特

定できず、試験用プログラムへ復帰することができないからである。従って、このような処理を行うことは、図２のマイクロコンピュータの構成では不可能であった。

【００２３】

【課題を解決するための手段】

前記課題を解決するために、本発明は、セキュリティ機能を有するマイクロコンピュータを、通常動作用のプログラムが格納された第１のメモリと、機能試験用のプログラムが格納された第２のメモリと、外部端子から与えられる信号を監視して試験モードが指定されたことを検出する試験モード検出回路と、前記試験モードが指定されていないときには前記第１のメモリにアクセスして前記通常動作用のプログラムを実行し、該試験モードが指定されたときには前記第２のメモリにアクセスして前記機能試験用のプログラムを実行するＣＰＵと、前記第１及び第２のメモリに対するアクセスアドレス及びデータを監視し、許可されていない不正なアクセスがあったときに前記ＣＰＵに対して特定の動作を実行させるメモリ管理ユニットと、前記試験モード時に前記ＣＰＵからセキュリティ試験信号が出力され、かつ特定のメモリ領域がアクセスされたときに、予め設定された特定の命令を該ＣＰＵに与える試験回路とで構成している。

【００２４】

本発明によれば、以上のようにマイクロコンピュータを構成したので、機能試験において次のような作用が行われる。

【００２５】

外部端子の信号で試験モードが入力されて試験モード検出回路で検出されると、ＣＰＵによって第２のメモリのプログラムが読み出され、機能試験が実行される。機能試験の内で、セキュリティ試験信号が出力され、更に特定のメモリ領域がアクセスされると、試験回路から予め設定された特定の命令がＣＰＵに与えられる。従って、例えば、この特定の命令を不正なアクセスを行うような命令にしておけば、その命令を実行した時点でメモリ管理ユニットからＣＰＵに特定の動作をさせるような制御が行われるはずである。もしも、特定の動作が行われなければ、メモリ管理ユニットが故障していることが判明する。

【００２６】

【発明の実施の形態】

図１は、本発明の実施形態を示すマイクロコンピュータの構成図であり、図２中の要素と共通の要素には共通の符号が付されている。

【００２７】

このマイクロコンピュータは、セキュリティ機能を有するもので、図２と同様のＣＰＵ１、ＲＯＭ２，３、ＲＡＭ４、周辺回路５、バス（またはブリッジ）６、セキュリティ回路７、及び試験モード検出回路９と、図２とは異なる試験用回路１０を備えている。

【００２８】

ＣＰＵ１は、ＲＯＭ２，３等のメモリに格納された命令を逐次実行するものである。ＲＯＭ２は、このマイクロコンピュータの主要な動作を決めるＯＳ等のプログラムを格納した読み出し専用のメモリであり、ＲＯＭ３は、チップの製造試験用のプログラム、セキュリティ用の最小限のライブラリ、ファンクションコール用のサブルーチン等を格納した読み出し専用のメモリである。

【００２９】

ＲＡＭ４は、データを格納したりプログラムを一時的に格納するためのメモリで、電気的に書き換え可能な不揮発性メモリも含まれる。周辺回路５は、暗号処理や外部との通信を行うための回路である。バス６は、ＣＰＵ１とその他のＲＯＭ２，３等との接続部分で、トライステートバスやＯＲバスといったバス接続やブロック間の論理やタイミングを調整するブリッジ回路が用いられる。

【００３０】

セキュリティ回路７は、メモリ管理ユニットとも呼ばれ、ＣＰＵ１が読み出したアドレスや命令を逐次監視し、実行や読み書きが許可されていないプログラム領域やデータ領域へのアクセスがあった場合に、ＣＰＵ１に対して不正アクセク検出信号ＩＬを出力して、適切な処理を行わせるための回路である。

【００３１】

試験モード検出回路９は、端子ＣＬＫ，ＲＳＴ，ＳＩＯから与えられる特定シーケンスの信号パターンによって、ＬＳＩが試験モードに設定されたことを検出

し、ＣＰＵ１に対する試験モード信号ＴＭをアクティブにするものである。通常の動作中に誤って試験モードに移行することがないように、端子ＣＬＫ，ＲＳＴ，ＳＩＯには、通常の動作では起こり得ない信号パターンを与えるようにしている。例えば、リセット（ＲＥＳ＝“Ｌ”）期間中に、端子ＣＬＫのクロックに同期して特定の信号パターンを端子ＳＩＯに与え、ＬＳＩのプログラムでその信号パターンを識別して試験状態に移行するような方法が採用されている。

【００３２】

試験用回路１０は、製造試験時にＣＰＵ１に試験用の命令を実行させ、アプリケーション・プログラムを正しく実行できるか否か、周辺回路５が正しく動作するか否か等を試験するための回路である。

【００３３】

この試験用回路１０は、レジスタ１１、セレクタ１２、アドレスデコーダ１３、及びＡＮＤ（論理積ゲート）１４を有している。レジスタ１１は、特定の命令コードを格納するものであり、セレクタ１２は、メモリ２～４から読み出されてバス６を介して出力された読み出しデータＲＤＴとレジスタ１１に格納された特定の命令を選択してＣＰＵ１に出力するものである。

【００３４】

アドレスデコーダ１３は、バス６から出力されるアドレスＡＤＲを解読して、ＲＯＭ２が選択されたときにその出力信号をアクティブにするものである。ＡＮＤ１４は、ＣＰＵ１から与えられるセキュリティ試験信号ＳＴとアドレスデコーダ１３の出力信号が共にアクティブになったときに、セレクタ１１をレジスタ１２側に切り替えるための切替信号を出力するものである。

【００３５】

図３及び図４は、図１の動作を示すフローチャート（その１、及びその２）である。以下、これらの図３及び図４を参照しつつ、図１の試験時の動作を説明する。

【００３６】

図３には、ＲＡＭ４に格納されたアプリケーション・プログラムから、分岐を禁止したＲＯＭ２上の領域へ分岐した際に、このＲＯＭ２上での命令実行を許可

してしまう故障の有無を試験するプログラムの処理手順が示されている。ここでは、アプリケーション・プログラムが格納されたＲＡＭ４のアドレスＡＰＰから、ＯＳが格納されたＲＯＭ２のアドレスＳＹＳへの分岐を許可した場合を想定している。

【００３７】

まず、端子ＣＬＫ，ＲＳＴ，ＳＩＯに、試験モードを設定するための信号パターンを印加する。これにより、試験モード検出回路９から出力される試験モード信号ＴＭがアクティブとなり、ＣＰＵ１によってＲＯＭ３に格納された試験プログラムの実行が開始される。

【００３８】

図３のステップＳ１において、ＣＰＵ１から出力されるセキュリティ試験信号ＳＴをアクティブにする。

【００３９】

ステップＳ２において、ＲＡＭ４のアプリケーション・プログラム内のアドレスＡＰＰに、ＯＳ内のアドレスＳＹＳへの分岐命令の命令コードを書き込む。これにより、ＣＰＵ１がアドレスＡＰＰの命令を実行すると、アプリケーション・プログラムからＯＳへの分岐処理が実現できるようになる。

【００４０】

ステップＳ３において、アプリケーション・プログラム内のアドレスＡＰＰでのプログラムの実行を禁止するように、セキュリティ回路７を設定する。

【００４１】

ステップＳ４において、スタックに試験プログラム中の故障判定ルーチン１の先頭アドレスＪＤＧ１をプッシュする。

【００４２】

ステップＳ５において、アドレスＡＰＰへ分岐する。具体的には、試験プログラムからアドレスＡＰＰへの分岐命令を実行する。これにより、ＣＰＵ１のプログラム・カウンタに値ＡＰＰが転送され、次の命令フェッチはアドレスＡＰＰから行われる。

【００４３】

ステップＳ６において、アドレスＡＰＰにはＯＳ内のアドレスＳＹＳへの分岐命令が格納されているので、ＣＰＵ１は続いてアドレスＳＹＳへの分岐命令を実行する。アドレスＳＹＳの命令フェッチが検出されると、試験用回路１０中のセレクタ１２は、レジスタ１１側に切り替えられる。これにより、レジスタ１１に格納されている特定の命令、例えばサブルーチン復帰命令がＣＰＵ１へ与えられる。ＣＰＵ１は、そのサブルーチン復帰命令をフェッチし、そのフェッチしたサブルーチン復帰命令を実行する。

【００４４】

ステップＳ７では、サブルーチン復帰命令の実行結果による例外状態の発生の有無が判定される。もしも、セキュリティ回路７またはその出力系統に故障があると、例外状態が発生しないのでステップＳ８へ進む。また、セキュリティ回路７が正常に動作していれば、例外状態が発生してステップＳ９へ進む。

【００４５】

ステップＳ８では、セキュリティ回路７の故障のために例外状態が発生しないので、サブルーチン復帰命令が実行され、スタックに格納された故障判定ルーチンＪＤＧ１がポップされてＣＰＵ１の命令実行が移行する。ステップＳ８の後、ステップＳ１０へ進む。

【００４６】

一方、ステップＳ９では、正常な動作として例外条件が発生し、予め定められた例外処理ルーチンへ分岐する。例外処理ルーチンでは、割り込みフラグを立てて例外状態の発生を記憶し、この例外処理ルーチンからの復帰命令を実行する。ステップＳ９の後、ステップＳ１０へ進む。

【００４７】

ステップＳ１０において、スタックには故障判定ルーチン１の先頭アドレスＪＤＧ１が格納されているので、ＣＰＵ１の命令実行は、この故障判定ルーチン１へ分岐する。

【００４８】

ステップＳ１１において、故障判定ルーチン１は、割り込みフラグの状態に応じて、故障の有無の判定結果を端子ＳＩＯを通して外部に出力する。即ち、割り

込みフラグが立っていれば故障がない旨の信号を出力し、割り込みフラグが立っていなければ故障がある旨の信号を出力する。これにより、セキュリティ回路７の故障の有無を知ることができる。

【００４９】

図４には、ＲＡＭ４に格納されたアプリケーション・プログラムから、分岐を許可したＲＯＭ２上の領域へ分岐した際に、ＲＯＭ２上での命令実行を禁止してしまう故障の有無を試験するプログラムの処理手順が示されている。ここでは、図３と同様に、アプリケーション・プログラムが格納されたＲＡＭ４のアドレスＡＰＰから、ＯＳが格納されたＲＯＭ２のアドレスＳＹＳへの分岐を許可した場合を想定しており、この図３中のステップと処理内容が同一のステップには、同一の符号が付されている。

【００５０】

図４の処理では、図３中のステップＳ３，Ｓ４，Ｓ７～Ｓ１１に代えて、それぞれ若干処理内容の異なるステップＳ３Ａ，Ｓ４Ａ，Ｓ７Ａ～Ｓ１１Ａを有している。

【００５１】

ステップＳ３Ａでは、アプリケーション・プログラム内のアドレスＡＰＰでのプログラムの実行を許可するように、セキュリティ回路７を設定する。

【００５２】

ステップＳ４Ａでは、スタックに試験プログラム中の故障判定ルーチン２の先頭アドレスＪＤＧ２をプッシュする。

【００５３】

ステップＳ７Ａでは、サブルーチン復帰命令の実行結果による例外状態の発生の有無が判定される。セキュリティ回路７が正常に動作していれば、例外状態が発生しないのでステップＳ８Ａへ進む。もしも、セキュリティ回路７またはその出力系統に故障があれば、例外状態が発生してステップＳ９Ａへ進む。

【００５４】

ステップＳ８Ａでは、正常な動作として例外状態が発生しないので、サブルーチン復帰命令が実行され、スタックに格納された故障判定ルーチンＪＤＧ２がポ

ップされてＣＰＵ１の命令実行が移行する。ステップＳ８Ａの後、ステップＳ１０Ａへ進む。

【００５５】

一方、ステップＳ９Ａでは、故障のために例外状態が発生し、予め定められた例外処理ルーチンへ分岐する。例外処理ルーチンでは、割り込みフラグを立てて例外状態の発生を記憶し、この例外処理ルーチンからの復帰命令を実行する。ステップＳ９Ａの後、ステップＳ１０Ａへ進む。

【００５６】

ステップＳ１０Ａにおいて、スタックには故障判定ルーチン２の先頭アドレスＪＤＧ２が格納されているので、ＣＰＵ１の命令実行は、この故障判定ルーチン２へ分岐する。

【００５７】

ステップＳ１１Ａにおいて、故障判定ルーチン２は、割り込みフラグの状態に応じて、故障の有無の判定結果を端子ＳＩＯを通して外部に出力する。即ち、割り込みフラグが立っていれば故障がある旨の信号を出力し、割り込みフラグが立っていなければ故障がない旨の信号を出力する。その他の処理は、図３と同様である。

【００５８】

このように、本実施形態のマイクロコンピュータは、次のような利点がある。

【００５９】

（１）　端子ＣＬＫ，ＲＳＴ，ＳＩＯ，ＶＤＤ，ＧＮＤ以外に、試験のための外部接続用端子や、チップ上の試験用パッドを必要としないので、悪意ある第３者によって、セキュリティの侵害が行われる危険性が少ない。

【００６０】

（２）　故障の有無で分岐先アドレスが異なるように構成しているので、セキュリティ回路７の試験を、不正アクセス検出信号ＩＬが“Ｌ”に固定された場合と、“Ｈ”に固定された場合の２通りの故障モードに対して行うことができる。

【００６１】

（３）　（２）の試験において、ＲＯＭ２上にあるＯＳ内部のプログラムを実行

することなく、ＲＡＭ４上にあるアプリケーション・プログラムの領域からＲＯＭ２への分岐の許可／禁止の試験ができる。従って、ＯＳの内容を知らなくても試験用のプログラムを作成することができる。

【００６２】

（４）　ＣＰＵ１やメモリ２～４は、従来どおりのものを用いることができるので、この発明を実施するために、既存の回路を変更する工数を最小限に抑えることができる。

【００６３】

なお、本発明は、上記実施形態に限定されず、種々の変形が可能である。

【００６４】

図５（ａ）～（ｄ）は、図１のマイクロコンピュータの変形例を示す図であり、いずれも上記実施形態と同様の利点を有している。

【００６５】

図５（ａ）のマイクロコンピュータは、バスとＣＰＵの間に試験用回路を設けるのではなく、メモリ（ＲＯＭ）の内部にセキュリティ回路の試験のためのセレクタを設け、通常動作時にはこのメモリから読み出されたデータを出力し、セキュリティ試験が指定されたときにはレジスタに格納された特定の命令を出力するように構成している。

【００６６】

図５（ｂ）のマイクロコンピュータは、ＣＰＵの内部に例外処理回路を設け、セキュリティ試験が指定され、かつ試験対象のメモリが選択されている時に、セキュリティ回路が不正アクセスを検出した場合に、例外状態を発生させるか特殊な動作モードへの移行を行うようにしている。

【００６７】

図５（ｃ）のマイクロコンピュータは、セキュリティ試験が指定され、かつ試験対象のメモリが選択されている時に、このメモリから読み出された命令のビットパターンに対し、“１”にしたいビットをＯＲゲートによって、“０”にしたいビットをＡＮＤゲートによって、置換を実現するものである。この回路では、通常動作時には、メモリから読み出されたデータが、ＡＮＤやＯＲを介してその

ままＣＰＵに与えられるようになっている。

【００６８】

図５（ｄ）のマイクロコンピュータは、セキュリティ試験が指定されたときに、メモリに対する制御信号がアクティブになることを禁止すると共に、トライステートバッファを用いて、レジスタからバスに特定の命令コードを出力するように構成している。

【００６９】

【発明の効果】

以上詳細に説明したように、本発明によれば、試験モード時にＣＰＵからセキュリティ試験信号が出力され、かつ特定のメモリ領域がアクセスされたときに、予め設定された特定の命令をこのＣＰＵに与える試験回路を有している。従って、第２のメモリに機能試験用のプログラムを予め格納しておくことで所定の機能試験が可能になり、試験用のパッドを設ける必要がなくなってセキュリティが向上する。更に、特定の命令として不正なアクセスを起こさせるような命令を設定しておけば、メモリ管理ユニットの動作確認も可能になるという効果がある。

【図面の簡単な説明】

【図１】

本発明の実施形態を示すマイクロコンピュータの構成図である。

【図２】

従来のマイクロコンピュータの一例を示す構成図である。

【図３】

図１の動作を示すフローチャート（その１）である。

【図４】

図１の動作を示すフローチャート（その２）である。

【図５】

図１のマイクロコンピュータの変形例を示す図である。

【符号の説明】

１　　ＣＰＵ

２，３　　ＲＯＭ

4　　ＲＡＭ

5　　周辺回路

6　　バス

7　　セキュリティ回路

9　　試験モード検出回路

１０　　試験用回路

１１　　レジスタ

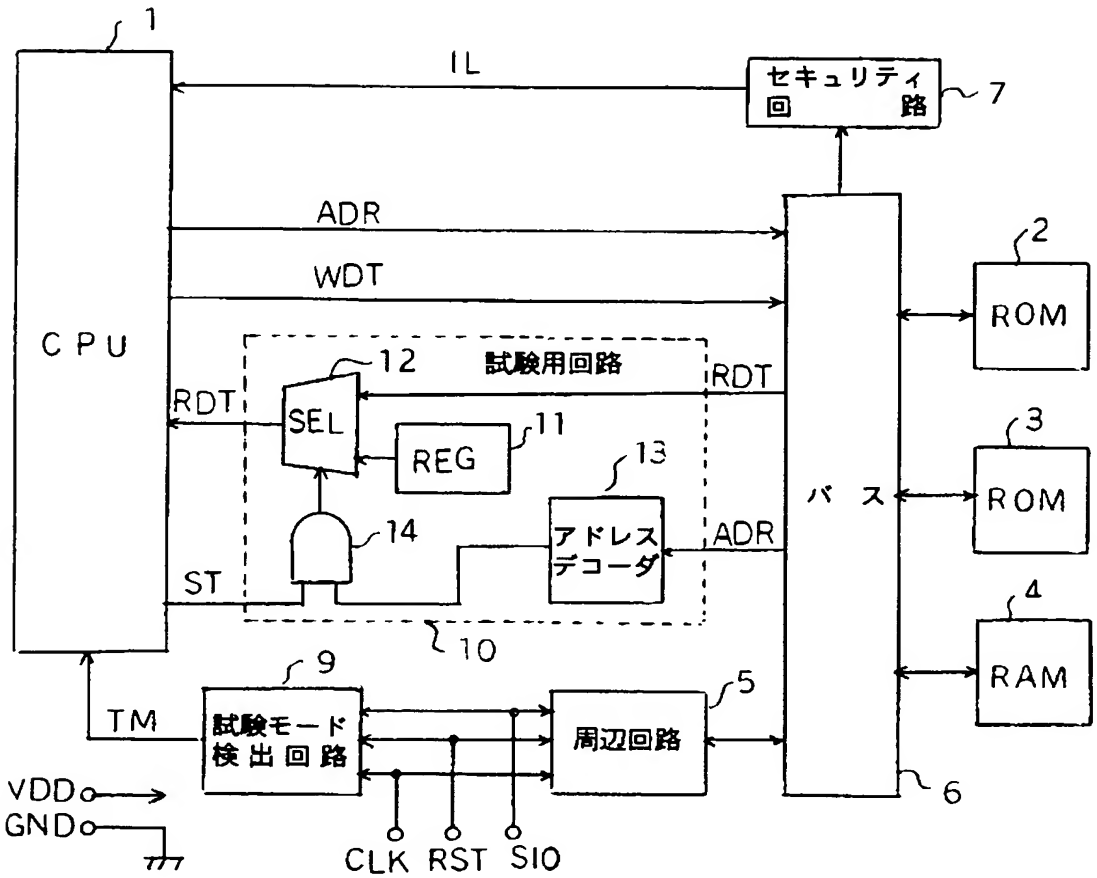
１２　　セレクタ

１３　　アドレスデコーダ

１４　　ＡＮＤ

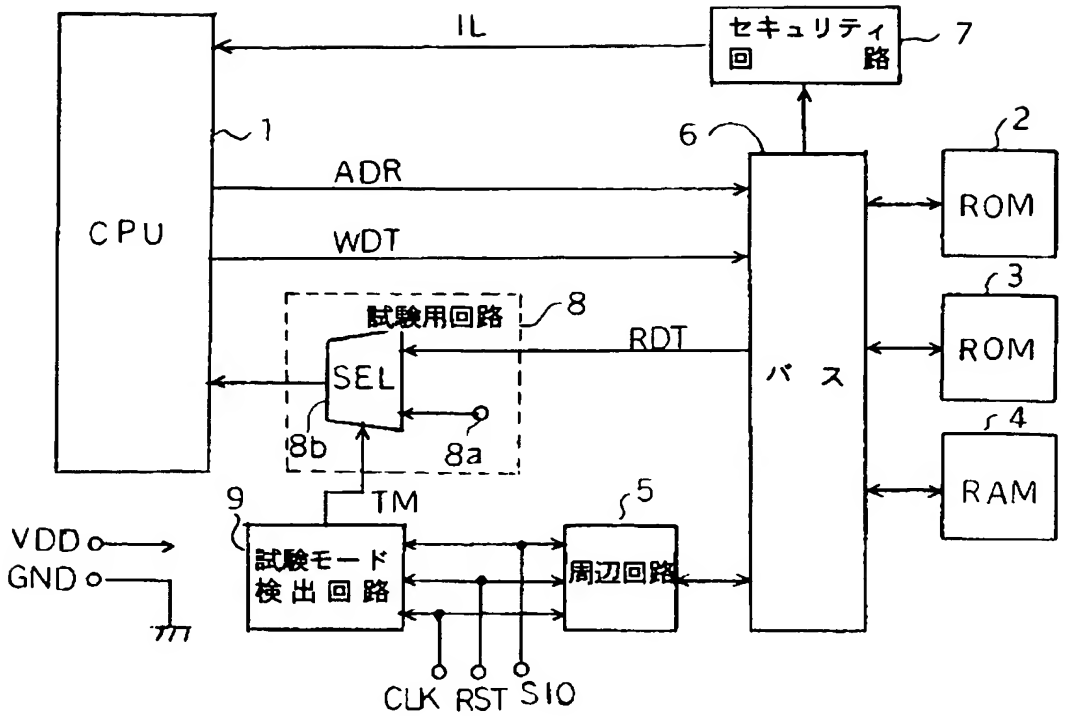
【書類名】　図面

【図１】



本発明の実施形態のマイクロコンピュータ

【図２】



従来のマイクロコンピュータ

【図３】

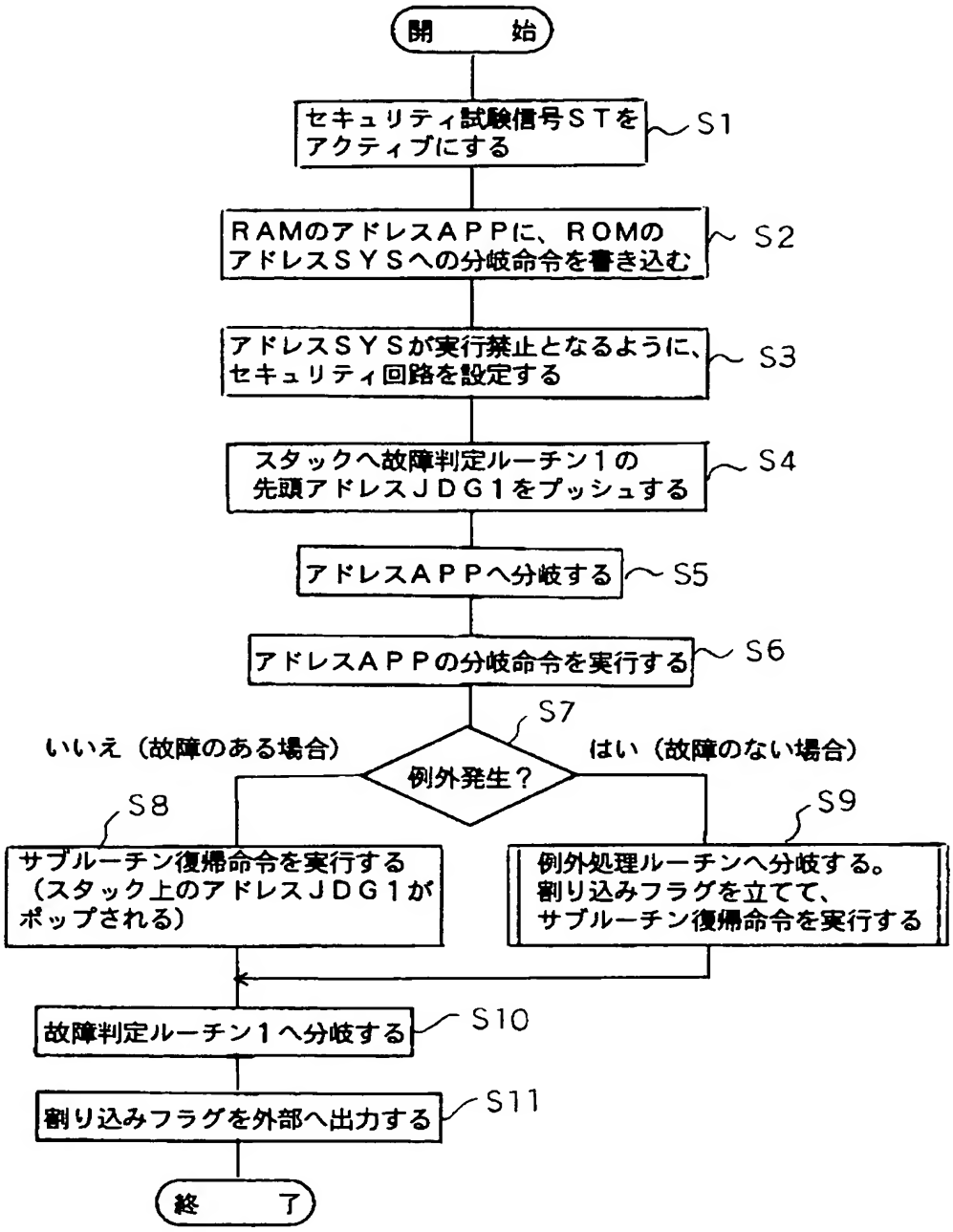

開　始
セキュリティ試験信号ＳＴをアクティブにする
S1
ＲＡＭのアドレスＡＰＰに、ＲＯＭのアドレスＳＹＳへの分岐命令を書き込む
S2
アドレスＳＹＳが実行禁止となるように、セキュリティ回路を設定する
S3
スタックへ故障判定ルーチン１の先頭アドレスＪＤＧ１をプッシュする
S4
アドレスＡＰＰへ分岐する
S5
アドレスＡＰＰの分岐命令を実行する
S6
S7
例外発生？
いいえ（故障のある場合）
はい（故障のない場合）
S8
サブルーチン復帰命令を実行する（スタック上のアドレスＪＤＧ１がポップされる）
S9
例外処理ルーチンへ分岐する。割り込みフラグを立てて、サブルーチン復帰命令を実行する
故障判定ルーチン１へ分岐する
S10
割り込みフラグを外部へ出力する
S11
終　了

図１の動作（その１）

【図４】

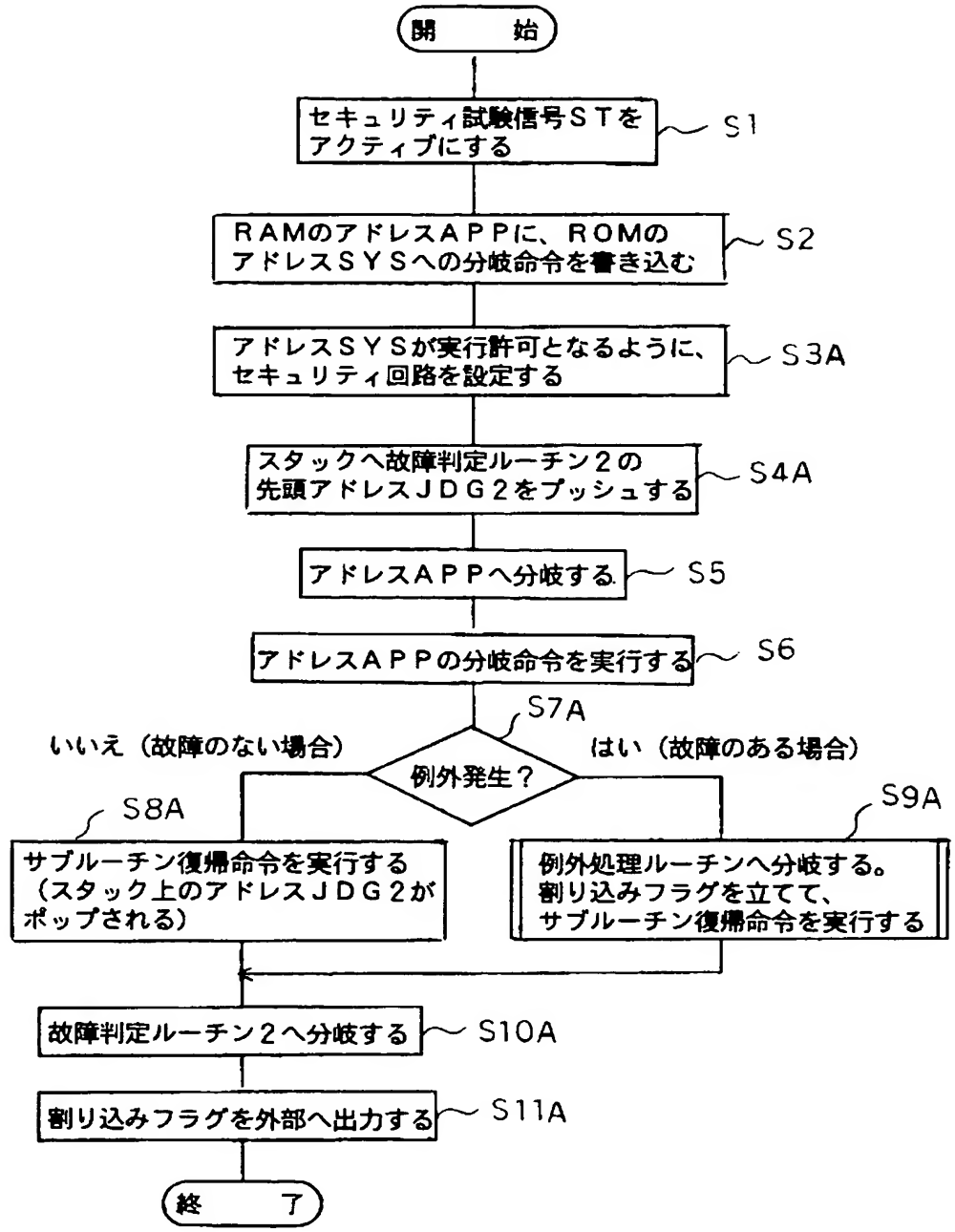

開　始
セキュリティ試験信号ＳＴをアクティブにする
S1
ＲＡＭのアドレスＡＰＰに、ＲＯＭのアドレスＳＹＳへの分岐命令を書き込む
S2
アドレスＳＹＳが実行許可となるように、セキュリティ回路を設定する
S3A
スタックへ故障判定ルーチン２の先頭アドレスＪＤＧ２をプッシュする
S4A
アドレスＡＰＰへ分岐する
S5
アドレスＡＰＰの分岐命令を実行する
S6
S7A
いいえ（故障のない場合）
例外発生？
はい（故障のある場合）
S8A
サブルーチン復帰命令を実行する（スタック上のアドレスＪＤＧ２がポップされる）
S9A
例外処理ルーチンへ分岐する。割り込みフラグを立てて、サブルーチン復帰命令を実行する
故障判定ルーチン２へ分岐する
S10A
割り込みフラグを外部へ出力する
S11A
終　了

図１の動作（その２）

【図５】

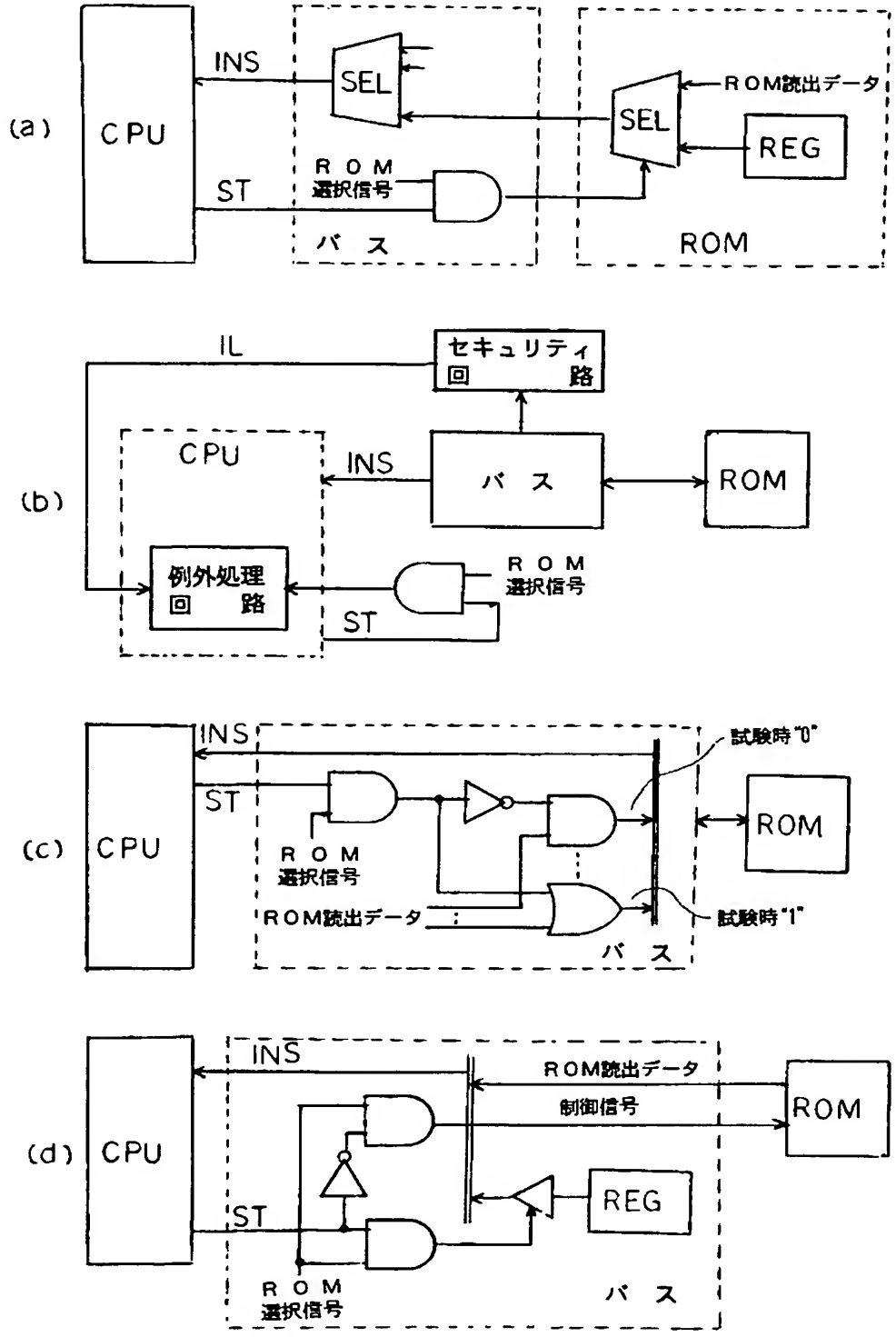


図１のマイクロコンピュータの変形例

【書類名】　　要約書

【要約】

【課題】　チップ上に試験用のパッドを設けずに、セキュリティ回路の機能を含む各種の自己試験ができるマイクロコンピュータを提供する。

【解決手段】　外部端子ＣＬＫ，ＲＳＴ，ＳＩＯから与えられる信号で試験モード信号ＴＭがアクティブにされると、ＣＰＵ１によってＲＯＭ３に格納された各種の自己試験プログラムが読み出されて実行される。試験プログラムでセキュリティ回路７の試験になると、セキュリティ試験信号ＳＴがアクティブとなり、更に所定のアドレスＡＤＲがアクセスされると、試験用回路１０のＡＮＤ１４の出力信号によってセレクタ１２がレジスタ１１側に切り替えられる。レジスタ１１には、例えば不正命令が設定されており、この不正命令がＣＰＵ１に与えられる。ＣＰＵ１が不正命令を実行した時に、不正アクセス検出信号ＩＬが出力されるか否かによってセキュリティ回路７の良否を判別する。

【選択図】　　図１

特願２００２－３５４７２６

出　願　人　履　歴　情　報

識別番号　　［０００００２９５］

１．変更年月日　　１９９０年　８月２２日
［変更理由］　　新規登録
住　所　　東京都港区虎ノ門１丁目７番１２号
氏　名　　沖電気工業株式会社